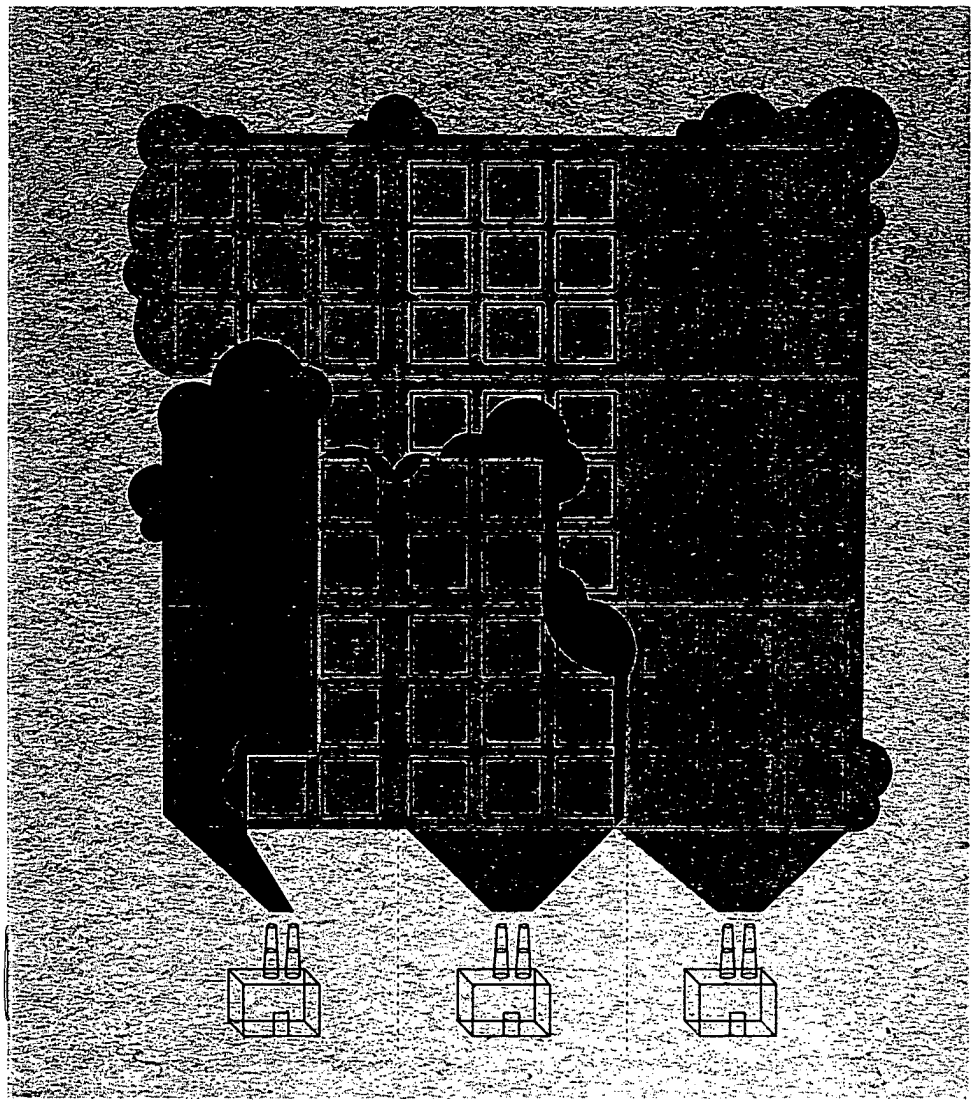
MARCH/APRIL 2006
VOLUME 3, NUMBER 2

Executive COUNSEL

C-TITLE INSIGHTS FOR BUSINESS LEADERS



NEW SQUEEZE ON EMPLOYERS

Accounting for Trade Secret Assets

Sarbanes-Oxley Requirements for the New Economy

By R. Mark Halligan and Richard F. Weyand

It's now widely accepted that Sarbanes-Oxley requires corporate officers and directors to have procedures in place to inventory, manage, track, and report on changes in the value of the company's trade secrets. This development stems directly from the definition of a trade secret, the increasing share of intangible assets in the market valuation of publicly held companies, and the purposes of the Sarbanes-Oxley legislation.

This article will explain how these factors combine to create an obligation for trade secret procedures, detail current developments in the legal and regulatory environment related to these obligations, and describe how satisfactory procedures can be effectively and efficiently implemented.

TRADE SECRETS

A trade secret is legally defined as information, including a formula, pattern, compilation, program device, method, technique, or process, that (1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means, by other persons who can obtain economic value from its disclosure or use, and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The fact that a trade secret is comprised of information makes it a unique asset within the company. Unlike physical assets, information can easily be duplicated without cost through the copying of documents or computer files. In addition, the loss of information through such duplication does not result in the loss of the original information. Where the theft of a physical asset, such as a company truck, requires the physical removal of the asset from the company, and the absence of the asset can be subsequently noted, the theft of a trade secret leaves no trace. The information is still there in the possession of the company. A simple audit will not reveal the loss.

The second aspect of the definition is what gives a trade secret independent economic value. The economic value derived from the information not being generally known quantifies the advantage it provides over competitors. This competitive advantage translates into real terms — net present value — because it represents the opportunity for future cash flow.

The third aspect of the definition predicates that value on efforts taken to maintain the secrecy of the information. If the information is revealed

through a failure to maintain its secrecy, the economic value derived from the information not being generally known is lost and the value of the trade secret is destroyed.

Thus the difficulty in crafting appropriate corporate procedures for trade secrets results directly from the nature of a trade secret itself. A trade secret is an information asset that can be surreptitiously stolen, and its value destroyed, while the information itself remains within the possession of the company.

THREATS TO TRADE SECRETS

Threats to trade secrets divide naturally into two types, external and internal. External threats include all means of determining the information from outside the company. Hackers, network attacks, competitive corporate intelligence, dumpster diving, bogus job applicants – every outside attempt to penetrate the company and obtain information is an external threat to the company's trade secret assets.

U. S. COMPANIES MUST NOW HAVE A TRADE SECRET ASSET-CONTROL COMMITTEE AND/OR A SPECIFIC CORPORATE OFFICER CHARGED WITH THE RESPONSIBILITY TO IDENTIFY, PROTECT AND VALUATE TRADE SECRET ASSETS ON A DAY-TO-DAY BASIS.

The defenses against external threats include the use of passwords, firewalls, dongles, document disposal procedures, building security, visitor badges, limitations on outsider access to sensitive areas, and other measures.

Internationally, an Information Security Management Systems (ISMS) regime has grown up around the British standards, 7799-1 and 7799-2. The former was formalized as an international standard in ISO 17799. In America, ISF, COBIT, and NIST standards address this area as well.

The result of these efforts is that external threats are no longer the primary source of loss of information assets by American companies. This shift in the primary threat source, which occurred in the mid-1990s, has been documented in several surveys of American companies regarding known information losses.

The internal threats against the company's trade secret information arise from the exposure of the information to employees, contractors, consultants, and vendors. This problem is less tractable, because the information must be exposed to these insiders to obtain the competitive advantage resulting from the trade secret asset. Whereas preventing any exposure to outsiders is the goal of every defense against external threats, locking the information away from the insiders who must use the trade secret information robs the trade secret of its value.

The insider threat is not an empty one, even for companies with low turnover rates, and ISMS procedures provide no defense. A low 15 percent employee turnover rate still results in three people leaving the firm every week for every thousand employees.

THE DOCTRINE OF FREE AND OPEN INFORMATION

According to U.S. law, all information is in the public domain, free to be used by anyone for any legal purpose, with a few exceptions. Credit, health and other personal information is covered by various privacy laws, including the Fair Credit Reporting Act and the Health Insurance Portability and Accountability Act. Government secrets are covered under various laws, such as the Official Secrets Act.

The exceptions to the free use of information that are related to company information are patents and trade secrets. All other company information, however obtained, can be freely and legally used by anyone.

Patenting every piece of information the company has is neither cost-effective nor possible. Patents must meet certain strict criteria. In addition, the invention and the best mode for practicing the invention must be disclosed in the patent application. Finally, the information reverts to the public domain upon the expiration of the patent, which usually occurs within twenty years.

Disclosure of the formulas for a company's best-selling products — such as Coca-Cola or Oreo cookies — and reversion of these formulas to the public domain within twenty years is clearly not in the company's interest. In contrast, trade secrets need not meet the patent tests for novelty, uniqueness, or non-obviousness, need not be disclosed, and need not revert to the public domain. A trade secret may be held forever.

The importance of trade secret protections to the company is now clear. Absent the protection of trade secret status, all unpatented information that the firm's employees gain from the company is legally theirs to use as they see fit upon leaving the firm.

THE BEST DEFENSE: EEA OR UTSA?

Given that people are free under the

law to use information freely for any legal purpose as long as it does not fall under one of the exceptions, the burden of proof is on the company to prove that information obtained from it qualifies under the trade secret exception. That is, there is ultimately no defense against the use of trade secret information by insiders except through civil litigation or criminal prosecution.

In 1996, Congress passed the Economic Espionage Act of 1996, which makes the theft of trade secrets, either to benefit foreign powers or for commercial and economic purposes, a federal criminal offense. The problem with the EEA is that it's a federal criminal statute with no private cause of action. "Prosecutorial discretion" governs whether an EEA criminal complaint or indictment will be issued to protect the public interest. Few cases have been prosecuted since the enactment of the EEA in 1996.

The standard of proof in a criminal proceeding is "beyond a reasonable doubt," a much higher standard than the "preponderance of the evidence" in civil trials. Also, the victim company is not entitled to recover damages under the EEA.

A civil action under the Uniform Trade Secrets Act (UTSA) enacted in some 46 states (with common law actions available in the remaining states) remains the best means of protecting trade secret assets. The UTSA provides for both compensatory damages and injunctive relief against the threatened or actual use of trade secrets. However, there are pitfalls in a civil action (discussed in the next section).

DEFENSE UNDER THE UTSA

In practice, there are four proofs under which the company must prevail in UTSA litigation in order to win protection for its information under the trade secrets exception.

The company must prove that (1) a trade secret exists, (2) the company has ownership rights in the trade secret information, (3) the company gave actual or constructive notice to the insider, and (4) the insider had access to the trade secret information.

The so-called EONA elements — Existence, Ownership, Notice, and Access — must all be proved if the company is to prevail in asserting the trade secrets exception and in obtaining protection against the unauthorized disclosure or use of its trade secret information The failure of proof by a preponderance of evidence on any one of the four proofs will result in a forfeiture of the trade secret information by the company.

The Existence element involves a consideration of the six factors set forth in the the Restatement (First) of Torts (1939), the foundation of the law of trade secrets in the United States. Of these six factors, the one that most often derails company trade secret assets is the absence of adequate security measures to guard the secrecy of the trade secret information.

The Ownership element requires that the company prove that it actually owns the trade secret information at issue. In contrast to the United States Copyright Act that contains a statutory work-for-hire provision, the UTSA contains no such statutory provision for the transfer of ownership of employee-developed trade secrets. Except in rare circumstances where an employee is hired to invent, trade secrets that are discovered or developed by employees belong to the employee absent the execution of a contractual assignment of such rights from the employee to the employer. At best, the employer obtains only a royalty-free "shop right" to practice the trade secret, but the ownership rights remain with the employee.

The Notice element relates to the overarching doctrine that information is open to use by all unless it falls into one of the intellectual property exceptions. The courts apply a "reasonable person" test to ascertain whether the insider knew, or had reason to know, that the information at issue was an employer-owned trade secret asset.

THE FIRST STEP IN ACCOUNTING FOR TRADE SECRETS IS TO STOP MAKING, REPEATING, LISTENING TO, OR COUNTENANCING ANY ARGUMENTS AS TO WHY IT CANNOT BE DONE. THAT'S OFF THE TABLE. THERE IS NO LONGER ANY WAY FOR THE CORPORATE DIRECTOR OR OFFICER TO IGNORE ACCOUNTING FOR OR PROTECTING A LARGE PORTION OF THE COMPANY'S CAPITALIZATION.

The Access element is necessary to show that the acquisition, disclosure or use took place improperly within a confidential relationship. A trade secret must not be readily ascertainable by proper means, and independent reverse engineering or independent development of the trade secret information is not actionable. It is the company's obligation to prove that such independent develop-

ment did not occur. Without knowledge of where within the company the trade secret information is known and where the employee has worked, this proof is very difficult.

The test of these four elements relates to prior actions, actions taken by the company before the misappropriation of the trade secret information by the insider. Security measures must already be in place. An agreement as to the ownership rights must already have been executed by the parties. The insiders must have been given reasonable notice that the information is a company trade secret. Tracking of trade secret information and insider activities is necessary to prove that the insider did not independently develop the information.

CAPITALIZATION, BOOK VALUE, AND LOSSES

The difference between the capitalization of publicly traded companies and their book values represents the value of their intangible assets. While these include patents, trademarks, branding, and goodwill, the bulk of these intangible assets is trade secrets. As we have seen, those trade secrets, absent proper stewardship by the company, are not defensible in court and are, in fact, free and open information that can be legally used by anyone.

The capitalization and book values of U. S. companies have been diverging over the last forty years. Whereas the book value of the company — its accounted physical assets — once constituted the majority of its shareholder value, the situation today is reversed. For some technology companies — with leased offices, furniture, and computer equipment — the value of their physical assets approaches zero.

Trade secrets define an asset class. Corporate asset valuations have shifted in the United States from physical property assets to intellectual property assets. Trade secret assets are estimated to comprise 80 percent of the assets in new economy companies. Ideas are now the core of value creation. Corporate growth is being driven by idea creations. The Financial Accounting Services Board (FASB 141 and 142) and the Internal Revenue Service (Section 482 Regulations) are beginning to develop rules and procedures for capturing the economic value of this new asset class.

Until recently, most companies neglected trade secret assets, and most companies do not have adequate systems in place for their identification, protection and economic valuation. Tens of billions of dollars in trade secret assets are lost each year by U.S. companies due to the failure to take reasonable steps to protect trade secret assets. (See, for example, the 2004 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.) The greatest losses to American companies are losses of R&D and manufacturing trade secret assets. Losses have averaged almost $50 million per incident.

NEW FIDUCIARY DUTIES

Companies have a fiduciary duty to their shareholders to identify and protect trade secret assets. Intangible property, intellectual asset management and information security are now critical flash points in the Sarbanes-Oxley Act of 2002 and a myriad of other federal and state statutes. At the heart of these developments, trade secret assets comprise the largest asset class of most U.S. corporations.

Until Sarbanes-Oxley, intellectual asset management was not viewed as an oversight issue for the boards of directors of U. S. companies. Management was given carte blanche authority over intellectual property matters. The board of directors became involved, if at all, only when the company was engaged in a major intellectual property lawsuit.

Sarbanes-Oxley changed the rules of the game. It's now clear that boards of directors and top management must become actively involved with intellectual asset management and information security issues to avoid civil and criminal liability under Sarbanes-Oxley, as well as shareholder derivative suits for the breach of the fiduciary duty to adequately protect intellectual property assets.

Sarbanes-Oxley imposes new duties of disclosure and corporate governance. Section 302 of the Act requires the CEO and CFO of public companies to certify that their annual and quarterly reports do not contain any untrue or misleading statements of material fact or material omissions and to certify that the financial information in the report fairly presents the financial condition of the company. Section 404 requires companies to document and certify the scope, adequacy and effectiveness of the internal control structure and procedures for financial reporting and controls. Section 906 imposes civil and criminal penalties for violations of Sarbanes-Oxley Act.

TRADE SECRETS AND SARBANES-OXLEY

Since trade secret assets are financial assets, Sarbanes-Oxley requires the economic valuation and financial reporting of such assets, with adequate internal controls and procedures for such reporting. At a minimum, U. S. Companies must now have a trade secret asset-control committee and/or a specific corporate officer charged with the

responsibility to identify, protect and valuate trade secret assets on a day-to-day basis.

These functions will also extend to third-party relationships and outsourcing in foreign countries. In addition, trade secret assets sold or acquired in mergers and acquisitions have to be tracked and monitored by the corporation.

The identification of trade secret assets requires a systematic procedure involving the six-factor test from the Restatement (First) of Torts, which we mentioned previously as part of the USTA Existence proof. These six criteria provide the litmus test for identifying trade secret assets.

Identification of trade secret assets also requires a classification scheme, because trade secret assets are "information" assets and such information can span a continuum, from notes on a blackboard to a secret formula locked in a safe. Seminars are now being held to develop "best practices" for company information classification systems and inventory procedures.

U.S. companies must also implement adequate security systems for the protection of trade secret assets. The trade secret owner must demonstrate that it has taken reasonable measures to protect those assets. In turn, security procedures implicate access controls and a wide array of other computer security issues, because most trade secret assets today are created, stored and disseminated in an electronic environment.

Access systems limit trade secret assets to disclosure or use on a "need to know" basis. This is the most effective way to protect trade secret assets. Password-protection and other security techniques must be used to define different levels of access. However, controlling access is just the first step. The company must also have tracking systems in place to control and monitor the distribution of trade secret assets after initial access.

These tracking systems for trade secret assets must insure that nondisclosure agreements are executed by third-party recipients before disclosure or use of the assets. The law requires that the third-party recipient be placed on notice and agree to receive the trade secret asset in confidence before third-party disclosure or use. Failure to obtain executed nondisclosure agreements from third-party recipients before disclosure of the trade secret assets will result in forfeiture and loss of those assets as a matter of law.

UNTIL SARBANES-OXLEY, INTELLECTUAL ASSET MANAGEMENT WAS NOT VIEWED AS AN OVERSIGHT ISSUE FOR THE BOARDS OF DIRECTORS OF U. S. COMPANIES.

VALUATION

Once systems are in place for the identification, classification and security of trade secret assets, economic valuation issues must be addressed. A recent ABA Section of Intellectual Property Law study concludes that the appropriate economic valuation model for trade secret assets is the *net present value of expected future cash flows* to be derived from the competitive advantages conferred by the trade secret asset.

This economic valuation model, in turn, is a function of both the content of the trade secret information and the stewardship and protection of the trade secret asset. Once again, if reasonable measures are not taken to protect the trade secret asset, then the trade secret rights in the asset will be forfeited and the economic value of the trade secret asset will be zero.

Identification, classification, security and economic valuation of trade secret assets is still not enough effort to ensure compliance with Sarbanes-Oxley. Adequate internal controls must also exist to assure the timely reporting of material changes or losses relating to trade secret assets. Management alerts must assure notice of material changes to trade secret assets for accurate financial reporting. The board of directors, in turn, must have oversight functions in place to make sure that it receives timely reports from management relating to trade secret assets.

HERE TO STAY

This is a tall order for U.S. companies and some might suggest that this takes Sarbanes-Oxley too far. Not so. The aggressive application of Sarbanes-Oxley will surely be one of the government's primary tools to protect U.S. companies from economic espionage and the theft of trade secret assets.

We have already seen evidence of these developments. For example, the SEC went on record last year to state that Sarbanes-Oxley and the concomitant SEC rules will "strengthen" the internal controls in U.S. companies for the identification and protection of trade secret assets which, in turn, will improve the ability of companies to track the costs and impact of economic espionage and trade secret thefts.

The focus of attention is now on the board of directors to ensure that management protects shareholder value. This trend started with the In Re Caremark shareholder derivative action in 1996. In 1994, Caremark was charged

with multiple felonies relating to violations of federal and state health care statutes. At issue was the scope of the fiduciary duty owed by the board of directors to shareholders. Although much of the decision is dicta, Caremark now stands for the proposition that the board of directors has a fiduciary duty to ensure that it is reasonably informed about the corporation's activities and to exercise good faith to ensure that adequate systems are in place to receive accurate and timely information so it can intervene to protect the interests of the shareholders and the corporation.

The principles of Caremark and Sarbanes-Oxley show up again in recent amendments to the Federal Sentencing Guidelines. The original 1991 guidelines did not specifically address directors. However, the new guidelines, effective November 1, 2005, "require boards of directors and executives to assume responsibility for the oversight and management of compliance and ethics programs." Trade secret assets and trade secret thefts now fall squarely within the Federal Sentencing Guidelines with the passage of the Economic Espionage Act of 1996. Compliance with Sarbanes-Oxley also falls within the ambit of the Federal Sentencing Guidelines. The Federal Sentencing Guidelines have become the universal de facto standard for all corporate compliance programs.

These changes in corporate governance relating to the identification and protection of trade secret assets are also manifested in the New York Stock Exchange's corporate governance rules effective October 31, 2004. The NYSE now mandates that reasonable measures be taken to protect trade secret assets and third-party proprietary and customer information.

IMPLEMENTATION

Having determined that an obligation for adequate internal controls for trade secrets information assets under Sarbanes-Oxley exists, we come to the question of how to implement such controls. The problem at first seems intractable, because the nature of trade secrets as an asset is so different from the physical assets that are routinely accounted. But many of the methods used to track physical assets can in fact be applied to trade secrets.

SINCE TRADE SECRET ASSETS ARE FINANCIAL ASSETS, SARBANES-OXLEY REQUIRES THE ECONOMIC VALUATION AND FINANCIAL REPORTING OF SUCH ASSETS, WITH ADEQUATE INTERNAL CONTROLS AND PROCEDURES FOR SUCH REPORTING.

The first step in accounting for trade secrets is to stop making, repeating, listening to, or countenancing any arguments as to why it cannot be done. That's off the table. There is no longer any way for the corporate director or officer to ignore accounting for or protecting a large portion of the company's capitalization. This corporate inaction is more egregious than negligently leaving the keys in the car. It is more akin to leaving the keys in the car together with a notarized transfer of title to the car on the dashboard. The first step in the development of a trade secrets accounting system is simply the commitment by the board of directors and key officers of the company to devote the time, effort and money necessary to accomplish this necessary task. Anything less, is now a violation of the Sarbanes-Oxley.

The next step in implementing a trade secrets identification and protection program should be to develop appropriate agreements to protect against the misappropriation of trade secrets by insiders and outsiders. These agreements should address trade secret identification issues, notice and ownership issues, and other issues necessary to maximize the protection of company trade secret information. These should not be boilerplate documents taken off the Internet or from canned software form programs. They need to be specifically tailored to the company's business operations and unique trade secret assets, and competent intellectual property counsel should be retained to assist in these critical tasks.

The trade secret inventory function is another important step that needs to be taken. The company must obtain a listing of what the trade secrets are. Automated methods are best for doing the initial data gathering. A web page on the company's intranet site can be used to solicit information from employees as to what the trade secrets of the firm are. You don't

IT'S NOW CLEAR THAT BOARDS OF DIRECTORS AND TOP MANAGEMENT MUST BECOME ACTIVELY INVOLVED WITH INTELLECTUAL ASSET MANAGEMENT AND INFORMATION SECURITY ISSUES.

need to spend millions of dollars on consultants to do this. Efforts are now underway to develop computer software systems to facilitate the inventory of trade secret assets in both large and small corporations.

Once such a listing is available, it is necessary to prioritize the trade secrets based on their value to the firm. Traditional accounting methods for physical assets do this already. Buildings, land and large equipment may be appraised annually. Furniture, personal computers, and vehicles are property-tagged and carried on a depreciation schedule. Pens, pencils, staplers, and coffee machines are expensed at purchase and are not tracked.

So with trade secrets. What are the critical trade secrets on which the company's future depends? At one time, gaining control of the company's vertical supply chain was considered important. It is now understood that companies are better off concentrating on their core competencies. What is not so well understood is that those core competencies derive directly from the company's trade secrets. The reason the company is better at those things than its competitors is that, at an institutional level, it knows how to do them, has specialized knowledge – it has trade secrets.

What are the company's core competencies? What are the trade secrets that comprise those core competencies?

Once the company's trade secrets list is prioritized, management needs to evaluate appropriate levels of security. The most important trade secret assets – those that comprise the company's core competencies, give the company its key competitive edge, and drive shareholder value – should have the highest security levels. Tracking these key trade secret assets is critical to trade secret protection, so that no argument of independent development can be successfully made.

A TRADE SECRET IS AN INFORMATION ASSET THAT CAN BE SURREPTITIOUSLY STOLEN, AND ITS VALUE DESTROYED, WHILE THE INFORMATION ITSELF REMAINS WITHIN THE POSSESSION OF THE COMPANY.

One key issue is restricting the knowledge of critical trade secrets within the company to those who have a need to know. If the company has a great new cookie recipe, the fellows who run the ovens don't need to know it. Contrariwise, if the company has a great new cooking process, the people who mix the dough don't need to know it.

Limiting the knowledge of critical trade secrets to the people who need to know them to do their jobs reduces the company's risk from employee turnover and increases the odds that any group of ex-employees will be able to put all of the pieces of the puzzle together.

When employees do leave, the exit interview needs to include a trade secrets portion, in which the employees are advised of the trade secret status of the critical information they have handled, and reminded of their obligations under the UTSA.

NO LONGER OPTIONAL

Trade secret assets can no longer be swept under the rug and ignored by management and the board until a key executive leaves the company and a lawsuit is filed. Failure to implement the systems outlined in this article – for the identification, classification, protection, valuation and oversight of trade secret assets – can no longer be tolerated. Continued failure to act will result in serious Sarbanes-Oxley violations, a rash of shareholder derivative suits and the could result in staggering losses of trade secret assets to competitors in the United States and abroad.

Trade secret accounting is in fact possible. More, in an age when the company's share value is driven by its information assets, it is necessary.

R. Mark Halligan is a trial lawyer and principal in the Chicago intellectual property law firm Welsh & Katz, Ltd. and a member of the adjunct faculty at John Marshall Law School in Chicago, where he teaches advanced trade secrets law. He is a frequent writer and lecturer on trade secrets law. He has sponsored the "Trade Secrets Home Page" on the Internet since 1994.

Richard F. Weyand is president of The Trade Secret Office, Inc., which is developing methods and software for the automated discovery, inventory, evaluation, and tracking of trade secret intellectual property assets. He has been an engineering professional in the computer and communications field since 1977, and has served as expert witness in trade secrets cases.